

A Note on the Isotopism of Commutative Semifields

Yue Zhou

*Department of Mathematics, Otto-von-Guericke-University Magdeburg,
39106 Magdeburg, Germany*

Abstract

We present an example of two isotopic but not strongly isotopic commutative semifields. This example shows that a recent result of Coulter and Henderson on semifield of order p^n , n odd, can not be generalized to the case n even.

Keywords:

commutative semifield, isotopism, planar function, projective plane

1. Introduction

A *semifield* F is an algebraic structure satisfying all the axioms for a skewfield except (possibly) associativity. A finite field is a trivial example of a semifield. Furthermore, if F does not necessarily have a multiplicative identity, then it is called a *presemifield*. A semifield is not necessarily commutative or associative. However, by Wedderburn's Theorem [21], in the finite case, associativity implies commutativity. Therefore, a non-associative finite commutative semifield is the closest algebraic structure to a finite field.

In the earlier literature, semifields were also called *division rings* or *distributive quasifields*. The study of semifields was initiated by Dickson [11], shortly after the classification of the finite fields. Until now, semifields have become an attracting topic in many different areas of mathematics, such as difference sets, coding theory and finite geometry.

The first non-trivial semifields were constructed by Dickson [11]. In [15], Knuth showed that the additive group of a semifield F is an elementary abelian group, and the additive order of the elements in F is called the characteristic of F . Hence, any finite semifield can be represented by $(\mathbb{F}_{p^n}, +, *)$.

Email address: yue.zhou@st.ovgu.de (Yue Zhou)

Here $(\mathbb{F}_{p^n}, +)$ is the additive group of the finite field \mathbb{F}_{p^n} and $x * y = \varphi(x, y)$, where φ is a mapping from $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ to \mathbb{F}_{p^n} .

On the other hand, there is a well-known correspondence, via coordinatisation, between commutative semifields and translation planes of Lenz-Barlotti type V.1, see [14]. In [1], Albert showed that two semifields coordinatise isomorphic planes if and only if they are isotopic:

Definition 1. Let $F_1 = (\mathbb{F}_{p^n}, +, *)$ and $F_2 = (\mathbb{F}_{p^n}, +, \star)$ be two presemifields. If there exist three linearized permutation polynomials $L, M, N \in \mathbb{F}_{p^n}[x]$ such that

$$M(x) \star N(y) = L(x * y)$$

for any $x, y \in \mathbb{F}_{p^n}$, then F_1 and F_2 are called *isotopic*, and the triple (M, N, L) is an *isotopism* between F_1 and F_2 . Furthermore, if there exists an isotopism of the form (N, N, L) between F_1 and F_2 , then F_1 and F_2 are *strongly isotopic*.

We refer the reader to [18] for more background on finite fields, in particular about linearized polynomials. Let $F = (\mathbb{F}_{p^n}, +, *)$ be a presemifield, and $a \in F$. If we define a new multiplication \star by the rule

$$(x * a) \star (a * y) = x * y,$$

we obtain a semifield $(\mathbb{F}_{p^n}, +, \star)$ with unit $a * a$. There are many semifields associated with a presemifield, but they are all isotopic.

Let $F = (\mathbb{F}_{p^n}, +, *)$ be a semifield. The subsets

$$N_l(F) = \{a \in F : (a * x) * y = a * (x * y) \text{ for all } x, y \in F\},$$

$$N_m(F) = \{a \in F : (x * a) * y = x * (a * y) \text{ for all } x, y \in F\},$$

$$N_r(F) = \{a \in F : (x * y) * a = x * (y * a) \text{ for all } x, y \in F\},$$

are called the *left*, *middle* and *right nucleus* of F , respectively. It is easy to check that these sets are finite fields. The subset $N(F) = N_l(F) \cap N_m(F) \cap N_r(F)$ is called the *nucleus* of F . It is easy to see, if F is commutative, then $N_l(F) = N_r(F) = N(F)$. In [14], the geometry interpretations of these nuclei are presented.

Next, we give the definition of planar functions, which was introduced by Dembowski and Ostrom in [10] to describe affine planes possessing a collineation group with specific properties.

Definition 2. Let p be an odd prime. A function $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ is called a *planar function*, or *perfect nonlinear (PN)*, if for each $a \in \mathbb{F}_{p^n}^*$, $f(x+a) - f(x)$ is a bijection on \mathbb{F}_{p^n} .

For $p = 2$, if x_0 is a root of $f(x + a) - f(x) = b$, then $x_0 + a$ is another one, hence there is no planar functions over \mathbb{F}_{2^n} . A *Dembowski-Ostrom* (DO) polynomial $D \in \mathbb{F}_{p^n}[x]$ is a polynomial

$$D(x) = \sum_{i,j} a_{ij} x^{p^i + p^j} .$$

Obviously, $D(x + a) - D(x) - D(a)$ is a linearized polynomial for any nonzero a . It can be proved that a planar DO polynomial is equivalent to a commutative presemifield with odd characteristic, see [9]. In fact, if $*$ is the presemifield product, then the corresponding planar function is $f(x) = x * x$; when the planar DO polynomial f is given, then the corresponding presemifield product can be defined as

$$x * y = \frac{1}{2}(f(x + y) - f(x) - f(y)) . \quad (1)$$

A function from a finite field \mathbb{F}_{p^n} to itself is *affine*, if it is defined by the sum of a constant and a linearized polynomial over \mathbb{F}_{p^n} . There are several equivalence relations of functions for which the *planar* property is invariant:

Definition 3. Two functions f and $g : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ are called

- *extended affine equivalent* (EA-equivalent), if $g = l_1 \circ f \circ l_2 + l_3$, where l_1, l_2 and l_3 are affine functions, and where l_1, l_2 are permutations of \mathbb{F}_{p^n} . Furthermore, if l_3 is the zero mapping, then f and g are called *affine equivalent*;
- *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent or graph equivalent), if there is some affine permutation L of \mathbb{F}_p^{2n} , such that $L(G_f) = G_g$, where $G_f = \{(x, f(x)) : x \in \mathbb{F}_{p^n}\}$ and $G_g = \{(x, g(x)) : x \in \mathbb{F}_{p^n}\}$.

Generally speaking, EA-equivalence implies CCZ-equivalence, but not vice versa, see [4]. However, if planar functions f and g are CCZ-equivalent, then they are also EA-equivalent [5, 16]. Because of the correspondence between commutative presemifields with odd characteristic and planar functions as we mentioned above, the strong isotopism of two commutative presemifields is equivalent to the affine equivalence of the corresponding planar DO functions, which we call directly the *equivalence* of planar DO functions.

2. Isotopism \neq Strong Isotopism

In [9], Coulter and Henderson proved the following theorem.

Theorem 1. *Let $F_1 = (\mathbb{F}_q, +, \star)$ and $F_2 = (\mathbb{F}_q, +, *)$ be isotopic commutative semifields. Then there exists an isotopism (M, N, L) between F_1 and F_2 such that either*

1. $M = N$, or
2. $M(x) \equiv \alpha \star N(x) \pmod{(x^q - x)}$, where $\alpha \in N_m(F_1) \setminus N(F_1)$ cannot be written in the form $\alpha = \gamma \star \beta^2$ where $\gamma \in N(F_1)$ and $\beta \in N_m(F_1)$.

It implies that any commutative semifield can generate at most two non-strongly isotopic commutative semifields. Some important corollaries are also presented in [9], for example,

Corollary 1. *Any two commutative semifields of order p^e with e odd are isotopic if and only if they are strongly isotopic.*

Pieper-Seier and Spille [20] showed that the Cohen-Ganley commutative semifield [8] has exactly two classes of strong isotopy. In this paper, we present another example¹.

First, we introduce a family of planar functions:

$$\frac{1}{2}(\text{Tr}(x^2) + G(x^{q^2+1}))$$

over $\mathbb{F}_{q^{2m}}$, where q is a power of an odd prime p , $m = 2k + 1$, $\text{Tr}(\cdot)$ is the trace function from $\mathbb{F}_{q^{2m}}$ to \mathbb{F}_{q^m} , and $G(x) = h(x - x^{q^m})$, where $h \in \mathbb{F}_{q^{2m}}[x]$ is defined as

$$h(x) = \sum_{i=0}^k (-1)^i x^{q^{2i}} + \sum_{j=0}^{k-1} (-1)^{k+j} x^{q^{2j+1}}.$$

This planar function family corresponds to Bierbrauer's generalization of the semifield discovered by Lunardon, Marino, Polverino and Trombetti over q^6 , see [2, 19]. Hence the corresponding semifield should be called Lunardon-Marino-Polverino-Trombetti-Bierbrauer (LMPTB) semifields [2].

¹In the previous version of this paper, we have claimed that our example is the first one. However, later Coulter and Knarr informed us about the result from [20]

Let $q = 3$, $m = 3$ and $\mathbb{F}_{3^6} = \mathbb{F}_3(\xi)$, where ξ is a root of $x^6 - x^4 + x^2 - x - 1 \in \mathbb{F}_3[x]$. Let $F_1 = (\mathbb{F}_{3^6}, +, \star)$ be the LMPTB semifield. By MAGMA[3], we calculate that $|N_m(F_1)| = 3^2$ and $|N(F_1)| = 3$, and there are four $\alpha \in N_m(F_1) \setminus N(F_1)$, which cannot be written in the form $\alpha = \gamma \star \beta^2$, where $\gamma \in N(F_1)$ and $\beta \in N_m(F_1)$. They are $\lambda, \lambda^3, \lambda^5$ and λ^7 , where $\lambda = \xi^{91}$.

Now, we can define another semifield F_2 with the multiplication given by

$$x \odot y = (\lambda \star x) \star y$$

Obviously, F_1 and F_2 are isotopic. As we mentioned above, to tell whether F_1 and F_2 are strongly isotopic, we just need to calculate whether $f_1(x) = x \star x$ is equivalent to $f_2(x) = x \odot x$. By Lagrange interpolation, we have

$$f_1(x) = x^{270} - x^{246} + x^{90} - x^{82} - x^{54} + x^{30} - x^{10} - x^2,$$

$$f_2(x) = \lambda^3(x^{270} - x^{246} - \lambda^2 x^{90} + \lambda^2 x^{82} - x^{54} + x^{30} + \lambda^2 x^{10} + \lambda^2 x^2) .$$

Let $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ be any function. Since the additive group of \mathbb{F}_{p^n} is the linear space \mathbb{F}_p^n , f can also be considered as a mapping from \mathbb{F}_p^n to itself. Define a matrix $M_f \in \mathbb{F}_p^{(2n+1, p^n)}$ as follows:

$$M_f = \begin{pmatrix} \cdots & 1 & \cdots \\ \cdots & x & \cdots \\ \cdots & f(x) & \cdots \end{pmatrix}_{x \in \mathbb{F}_p^n} \quad (2)$$

Then we can construct a linear code C_f over \mathbb{F}_p by the generator matrix M_f . Furthermore, it can be proved that

Proposition 1. *Let p be a prime, and n be an integer. Two functions $f, g : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ are CCZ-equivalent, if and only if the corresponding codes C_f and C_g are permutation equivalent.*

PROOF. Assume that C_f and C_g are permutation equivalent, then we have a permutation matrix P and a $(2n+1) \times (2n+1)$ matrix L with full rank, such that

$$L \cdot M_f \cdot P = M_g .$$

That means there are $u, v \in \mathbb{F}_p^n$ and a matrix \tilde{L} with full rank, such that

$$\tilde{L} \cdot \begin{pmatrix} \cdots & x & \cdots \\ \cdots & f(x) & \cdots \end{pmatrix} \cdot P = \begin{pmatrix} \cdots & x & \cdots \\ \cdots & g(x) & \cdots \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix} .$$

Therefore, by the definition of CCZ-equivalence, f and g are CCZ-equivalent. The proof of the converse is the same. \square

For the equivalence of codes, including permutation equivalence and monomial equivalence, see [13].

It is well-known that function f mapping \mathbb{F}_{p^n} to itself is planar if and only if for every nonzero $a \in \mathbb{F}_{p^n}$, the function $\text{Tr}(af(x))$ is generalized bent, see [7]. For planar DO-polynomials, it is equivalent to the nonsingularity of $\text{Tr}(af(x))$ as a p -ary quadratic form, for every nonzero $a \in \mathbb{F}_{p^n}$. Therefore, the weight distribution of C_f can be deduced, see [17], and there are only $p - 1$ code words (i, i, \dots, i) with weight p^n ($0 < i < p$). Thus, for the codes C_f and C_g from the planar functions f and g , monomial and permutation equivalence are identical. By MAGMA, we calculated that C_{f_1} is not monomially equivalent to C_{f_2} (MAGMA only offers the command to tell the monomial equivalence of two linear codes, that is why we emphasize the identity of monomial and permutation equivalence between C_f and C_g). Therefore, F_1 is not strongly isotopic to F_2 , which means that it is possible to construct inequivalent planar functions from known ones by the isotopism of corresponding presemifield.

Remark 1. For Dickson [11], Albert [1], Ganley [12] and Cohen-Ganley [8] commutative semifields, we did not find such λ to construct affine-inequivalent functions f_1 and f_2 as defined above on $\mathbb{F}_{3^{2m}}$, where $m = 2, 3$. For the Budaghyan-Helleseth-Bierbrauer (BHB) semifields [2, 5, 6] of order 3^6 , such λ can also be found. For any other larger m , it is beyond our computation capacity.

Remark 2. We find that f_2 is equivalent to the planar function from BHB semifield of order 3^6 , which means BHB semifield and LMPTB semifield of order 3^6 are isotopic but not strongly isotopic.

Acknowledgement

We are grateful to R. Coulter and R. Knarr for pointing out the result in [20].

References

- [1] A. Albert, Finite division algebras and finite planes, in: Combinatorial Analysis: Proceedings of the 10th Symposium in Applied Mathematics, volume 10 of *Symposia in Appl. Math.*, American Mathematical Society, Providence, R.I., pp. 53–70.

- [2] J. Bierbrauer, New commutative semifields from projection mappings, 2009. Manuscript, presented at the Colloquium on Combinatorics 2009, Magdeburg, Germany.
- [3] W. Bosma, J. Cannon, C. Playoust, The MAGMA algebra system I: the user language, *J. Symb. Comput.* 24 (1997) 235–265.
- [4] L. Budaghyan, C. Carlet, A. Pott, New classes of almost bent and almost perfect nonlinear polynomials, *IEEE Transactions on Information Theory* 52 (2006) 1141–1152.
- [5] L. Budaghyan, T. Helleseht, New perfect nonlinear multinomials over $F_{p^{2k}}$ for any odd prime p , in: SETA '08: Proceedings of the 5th international conference on Sequences and Their Applications, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 403–414.
- [6] L. Budaghyan, T. Helleseht, New commutative semifields defined by new PN multinomials, *Cryptography and Communications* (2010). Available online.
- [7] C. Carlet, S. Dubuc, On generalized bent and q -ary perfect nonlinear functions, in: *Information Theory and Communications Workshop*, 1999. Proceedings of the 1999 IEEE, p. 92.
- [8] S. Cohen, M. Ganley, Commutative semifields, two-dimensional over their middle nuclei, *Journal of Algebra* 75 (1982) 373–385.
- [9] R.S. Coulter, M. Henderson, Commutative presemifields and semifields, *Advances in Mathematics* 217 (2008) 282 – 304.
- [10] P. Dembowski, T. Ostrom, Planes of order n with collineation groups of order n^2 , *Mathematische Zeitschrift* 103 (1968) 239–258.
- [11] L. Dickson, On commutative linear algebras in which division is always uniquely possible, *Transaction of the American Mathematical Society* 7 (1906) 514–522.
- [12] M. Ganley, Central weak nucleus semifields, *European Journal of Combinatorics* 2 (1981) 339–347.
- [13] W.C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

- [14] D. Hughes, F. Piper (Eds.), Projective Planes, Springer, Berlin, 1973.
- [15] D. Knuth, Finite semifields and projective planes, Ph.D. thesis, California Institute of Technology, Pasadena, California, 1963.
- [16] G.M. Kyureghyan, A. Pott, Some theorems on planar mappings, in: WAIFI '08: Proceedings of the 2nd international workshop on Arithmetic of Finite Fields, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 117–122.
- [17] C. Li, L. Qu, S. Ling, On the covering structures of two classes of linear codes from perfect nonlinear functions, IEEE Transactions on Information Theory 55 (2009) 70–82.
- [18] R. Lidl, H. Niederreiter, Finite fields, Cambridge University Press, Cambridge ; New York :, 2nd edition, 1997.
- [19] G. Lunardon, G. Marino, O. Polverino, R. Trombetti, Symplectic spreads and quadric Veroneseans, 2009. Manuscript.
- [20] I. Pieper-Seier, B. Spille, Remarks on the paper: "on strong isotopy of dickson semifields and geometric implications", Results in Mathematics. Resultate der Mathematik 35 (1999) 310–313.
- [21] J.H.M. Wedderburn, A theorem on finite algebras, Transaction of the American Mathematical Society 6 (1905) 349–352.